Nicole MONTENEGRO

Définition

Lacinpic

Propriétés

À retenir

# Arithmétique 2

Les congruences

Nicole MONTENEGRO

Septembre 2017

# Sommaire

Maths pour l'informatique en SIO Nicole

MONTENEGRO Définition

Définition

Exemple Exemple

À retenir

Propriétés

À retenir

Nicole MONTENEGRO

Définition

Exemple

Propriété

À retenir

Vous passez l'épreuve de SI9 (Compétences artistiques) à l'oral devant un des 9 jurys.

Vous êtes le candidat nº 331 sur la liste.

Avec quel jury (numéroté de 1 à 9) allez vous passer?

Votre copain nº 286 est il sur le même jury?

Nicole MONTENEGRO

### Définition

Exemple

Propriété

À retenir

$$331 = 36 \times 9 + 7$$
$$331 - 286 = 9 \times 5$$

331 - 7, 331 - 16 et 331 - 286 sont des multiples de 9. 331 est à plusieurs multiples de 9 (pas de 9) des entiers 7, 286 et 16.

Nicole MONTENEGRO

#### Définition

Exemple

Propriétés

À retenir

# Définition

Soient a et b deux entiers. Soit p un entier,  $p \ge 2$ . On dit que

a est congru à b modulo p si a-b est un multiple de p.

On note alors

$$a \equiv b[p]$$
 ou encore  $a \equiv b \mod p$ .

# Sommaire

Maths pour l'informatique en SIO Nicole

MONTENEGRO Définition

Définition

Exemple

Propriétés Exemple

À retenir

Propriétés

À retenir

# MONTENEGRO

Définition

À retenir

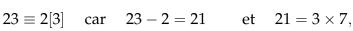
Exemple

 $23 \equiv -1[3]$  car 23 - (-1) est multiple de 3.

 $17 \equiv 8[3]$  car 17 - 8 = 9, et 9 est multiple de 3,









Nicole MONTENEGRO

Définition

Exemple

Propriétés

Propriétés

À retenir

# Propriété

a est congru à b modulo n si a et b ont même reste dans la division euclidienne par n.

### Nicole MONTENEGRO

Définition

Exemple

À retenir

# On remarquera que a est un multiple de b ssi $a \equiv 0[b]$ . Ainsi,

a est pair ssi  $a \equiv 0[2]$ .

*a* est multiple de 5 ssi  $a \equiv 0[5]$ .

#### Nicole MONTENEGRO

Définition

Exemple

•

À retenir

# Applications:



Une puce se trouve sur la case 0 d'un plateau circulaire de 12 cases.

- 1. Supposons qu'elle ait avancé de 15 sauts de 2 cases ; sur quelle case va-t-elle se poser ?
- 2. Si elle a fait 31 sauts de 3 cases, où atterit-elle?

#### Nicole MONTENEGRO

Définition

Exemple

Propriétés

1

À retenir

- 1. Supposons qu'elle avance par sauts de 2 cases; sur quelles cases va-t-elle se poser?
- 2. Si elle fait des sauts de 3 cases, quelles sont les cases qu'elle occupera?
- 3. Peut-elle passer sur toutes les cases du plateau autrement qu'avec des sauts de 1 case?
- 4. Si le plateau comportait 15 cases, quels sauts lui permettraient de visiter chaque case?

# Sommaire

Maths pour l'informatique en SIO Nicole

MONTENEGRO Définition

Définition

Exemple

Propriétés

À retenir

Exemple

Propriétés

À retenir

Nicole MONTENEGRO

Définition

Propriétés

À retenir

# Propriété

La relation de congruence modulo p est compatible avec les opérations algébriques usuelles :

 $Si \ a \equiv b[p] \ et \ a' \equiv b'[p] \ alors$ 

$$a + a' \equiv b + b' [p]$$

$$n \times a \equiv n \times b [p]$$

$$a \times a' \equiv b \times b' [p]$$

$$a^{k} \equiv b^{k} [p]$$

pour tout entier n et pour tout entier naturel non nul k.

# Nicole MONTENEGRO

Définition

Propriétés

À retenir

# Exemples:

Quel est le reste dans la division euclidienne par 6 de  $2015^{2015}$ ?

$$2015 = 335 \times 6 + 5$$

donc 
$$2015 \equiv 5[6]$$

$$2015^{2015} \equiv 5^{2015} [6$$

Nicole MONTENEGRO

Définition

Examela

Exemple

Propriétés

À retenir

# Exemples:

Quel est le reste dans la division euclidienne par 6 de 2015<sup>2015</sup>?

$$2015 = 335 \times 6 + 5$$

donc 
$$2015 \equiv 5[6]$$

Par compatibilité de la relation de congruence avec 14 puissance,

$$2015^{2015} \equiv 5^{2015} [6$$

Nicole MONTENEGRO

Définition

Propriétés

À retenir

# Exemples:

Quel est le reste dans la division euclidienne par 6 de  $2015^{2015}$ ?

$$2015 = 335 \times 6 + 5$$

donc 
$$2015 \equiv 5[6]$$

Par compatibilité de la relation de congruence avec la puissance,

$$2015^{2015} \equiv 5^{2015}[6]$$

# mais aussi l'informatique en $2015^{2015} \equiv (-1)^{2015} [6]$ SIO Nicole MONTENEGRO car $5 \equiv -1[6]$ Définition Propriétés À retenir

4□ > 4回 > 4 亘 > 4 亘 > □ ● のQで

15/24

Maths pour

# Maths pour mais aussi l'informatique en $2015^{2015} \equiv (-1)^{2015} [6]$ SIO Nicole MONTENEGRO car $5 \equiv -1[6]$ Définition or $(-1)^{2015} = -1$ Propriétés À retenir 4□ > 4回 > 4 亘 > 4 亘 > □ ● のQで 15/24

# Maths pour mais aussi l'informatique en $2015^{2015} \equiv (-1)^{2015} [6]$ SIO Nicole MONTENEGRO car $5 \equiv -1[6]$ Définition or $(-1)^{2015} = -1$ Propriétés À retenir donc $2015^{2015} \equiv -1[6]$ 4□ > 4回 > 4 = > 4 = > = 9 < @</p>

15/24

# Maths pour mais aussi l'informatique en SIO Nicole MONTENEGRO Définition orPropriétés À retenir donc ou reste est égal à 5.

 $2015^{2015} \equiv (-1)^{2015} [6]$ car  $5 \equiv -1[6]$ 

 $(-1)^{2015} = -1$ 

 $2015^{2015} \equiv -1[6]$ 

 $2015^{2015} \equiv 5[6]$ Dans la division euclidienne par 6 de  $2015^{2015}$ , le

<ロ > < 回 > < 回 > < 巨 > < 巨 > 豆 の < ○

15/24

### Nicole MONTENEGRO

Définition

Exemple

Propriétés

À retenir

Un entier est pair si son chiffre des unités est pair.\*

En effet, si  $n \in \mathbb{N}$ ,

$$n = a_k 10^k + \ldots + a_2 10^2 + a_1 10 + a_0$$

où  $a_0$  est le chiffre des unités,  $a_1$  celui des dizaines,  $a_2$  celui des centaines ...

$$10^k \equiv 0[2]$$

$$10^2 \equiv 0[2]$$

$$10 \equiv 0[2]$$

Donc

$$n\equiv a_0[2] \ !^*$$

# Nicole MONTENEGRO

Définition

Escaman 1a

Exemple

Propriétés

À retenir

Un entier est multiple de 9 si la somme de ses chiffres est multiple de 9.

$$10 \equiv 1[9] \Rightarrow 10^{2} \equiv 1^{2}[9]$$

$$\Rightarrow 10^{2} \equiv 1[9]$$

$$\Rightarrow 10^{3} \equiv 1^{3}[9]$$

$$\Rightarrow 10^{3} \equiv 1[9]$$

$$\cdots$$

$$\Rightarrow 10^{k} \equiv 1[9]$$

### Nicole MONTENEGRO

Définition

г 1

Propriétés

À retenir

# Ainsi, pour

$$n = a_k 10^k + \ldots + a_2 10^2 + a_1 10 + a_0$$

$$n \equiv a_k + \ldots + a_2 + a_1 + a_0[9]$$
!

Un entier est congru à la somme de ses chiffres modulo 9.

Si cette somme est multiple de 9, cet entier le sera aussi.

Nicole MONTENEGRO

Définition

г 1

Exemple Propriétés

À retenir

Le nombre 6 439 817 263 459 653 est il divisible par 9?

MONTENEGRO

Propriété

Modulo n, les multiples de a sont les multiples du PGCD(a, n).

Les multiples de 2 modulo 12 sont les multiples de

PGCD(2,12) c'est à dire les multiples de 2 : 0, 2, 4, 6,

Définition

Propriétés À retenir

8, 10

Les multiples de 3 modulo 12 sont les multiples de

PGCD(3,12) c'est à dire les multiples de 3 : 0, 3, 6, 9

Les multiples de 5 modulo 12 sont les multiples de PGCD(5,12) c'est à dire les multiples de 1 : 0, 1, 2, 3,

...11

◆□ ▶ ◆□ ▶ ◆ □ ▶ ◆ □ ◆ の ○ ○

20/24

# Sommaire

Maths pour l'informatique en SIO Nicole

MONTENEGRO

Définition

Exemple

À retenir

À retenir

Propriétés

Exemple

# Nicole MONTENEGRO

Définition

Exemple

Lacinpic

À retenir

# Soient a et b deux entiers. Soit p un entier, $p \ge 2$ . On dit que

a est congru à b modulo p si

Notation:

Nicole MONTENEGRO

Définition

Evennle

Propriátác

.

À retenir

Quel lien existe-t-il entre la relation de congruence et le reste dans la division euclidienne?

Nicole MONTENEGRO

Définition

Evomplo

Propriétés

À retenir

La relation de congruence modulo p est compatible avec les opérations algébriques usuelles :